For Electronic Posting…

Sorry, if you missed the talk you missed a pretty detailed whiteboard discussion! There's LOTS to know here, and I didn't want to make everyone's eyes bleed with a 110 slide PPT presentation. What's in here however is enough to get you started on Googling and reading. See the final slide for some references.

Also check out the Radware ERT report for a great reference on DDoS:

https://www.radware.com/PleaseRegister.aspx?returnUrl=6442459121

DDoS

Oct 2017 DC919 Meetup

Patrick McNeil

Why I’m qualified to talk about this…

- I’m on LinkedIn so just look me up if you care
- What’s relevant for this talk - Feb 2014 to Jun 2016 at Radware as a Carrier Solutions Architect
  - Worked with service providers such as those that rhyme with [Censored], and others…
  - Architecture design, lab testing, pilot testing in production, operational support and tuning, some incident response

DoS vs DDoS?

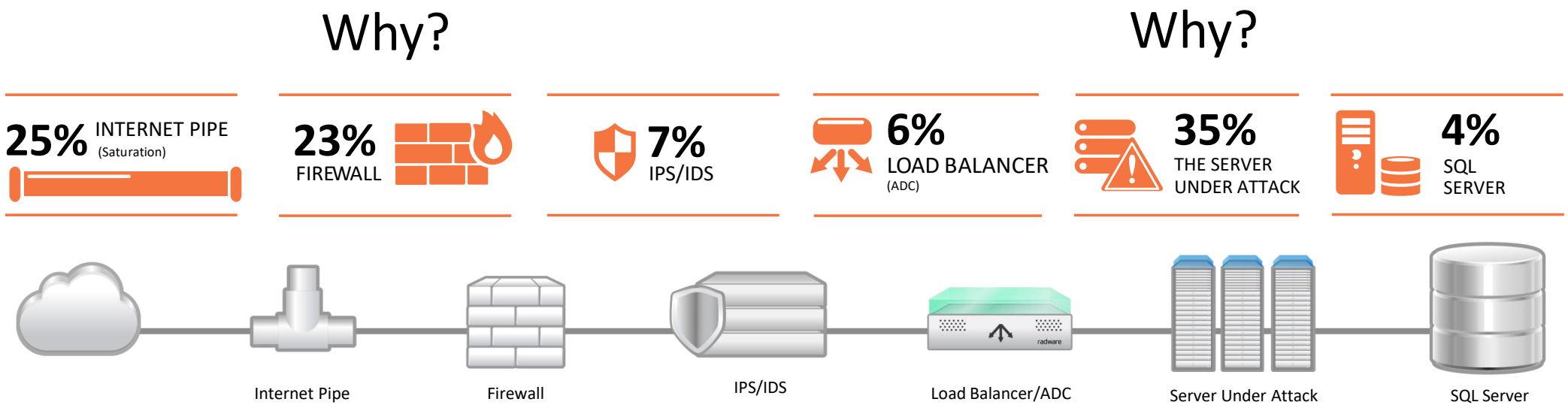
Facts from Radware 2016/2017 ERT Report

- 600 respondents from a variety of industries with a good sampling of engineers up to CISOs and worldwide geographies
- 34% of respondents had suffered a DDoS attack
- 83% deal with periodic or frequent low volume floods that impact performance or capacity
- Only 38% had calculated the cost of an attack. Of those who did, they found when hit they were about 50% “off” in their calculation

Motivations

- “Hactivism”
- Ransom - Armada collective, DD4BC (DDoS for Bitcoin) and LOTS of copycats
  - #1 motive (49%) according to Radware 2016/2017 ERT Report
- Distraction from other attacks - typically highly targeted and pre-exploited
- Gaming booters
- General mischief – ex: against your school to avoid an online test

DDoS Impacts



Source: Radware's 2016-2017 Emergency Response Team Report

Attack Evolution

- Simple floods
- Multi-vector, preceded by some fingerprinting
- Application specific torture/fuzzing/targeted floods
- Fast burst attacks – why?
- IOT driven is the new hotness

Attack Types

- Basic flood – from a single IP, hard to process traffic
- Reflection - single spoofed source IP, fired at lots of targets that then reply to your victim
- Amplification - Form of reflection where the response is significantly larger than the request, uses an open service
- Reflection and Amplification destinations can be opportunistic - you have a list of misconfigured hosts OR compromised hosts with purposeful misconfigurations
- Bots that you just task via C&C for a directed attack. IoT botnets have finally driven more attacks over 1 Tbps where they used to be in the 10s or 100s of Gigs. Mirai being the biggest driver and numerous variants.

Methods

- Simple network
  - TCP SYN most popular - spoofed source IP right at target
  - “Junk” packets for service that isn’t even running (ex: TCP STOMP from Mirai)
  - ACK or RST – spoof the message OR send SYN to lots of real sources w/source spoofed, reply goes to victim
  - UDP it's DNS, SNMP, SSDP, NTP, or chargen reflection / amplification
  - For amplification you need an open server port that responds to anyone's queries - produces large query result and returns to spoofed source IP
  - GRE floods - generic routing encapsulation
  - "SSL" renegotiation – keep changing ciphers, very CPU intensive
- Application
  - HTTP, HTTPS most common - flood, retrieve large file, slow connection, HTTPS hard to analyze
  - DNS "water torture" or recursive flood – lots of garbage hosts/subdomains

TOOLZ

- Started w/GUI tools like LOIC and HOIC, HOIC HTTP focused, LOIC TCP/UDP
- LOTS of other tools and scripts ranging from straight forward to ones that will use VPNs or Tor
- Moving to portal hosted on dark web somewhere or on a VPS but back-end server controlling the botnet is somewhere else. Hosting companies struggling to deal with outbound DoS. Scripts popular for these because of SSH access via mobile

DDoS Mitigation Process

- Identification / classification
  - Homegrown stats, netflow, openflow, detectors, in-line, “micro detection”
- Traffic redirection
  - DNS and ACL
  - BGP - smaller prefix, path prepend, owner withdrawal, single IP on owned networks, BGP flowspec
- Mitigation
- Clean Traffic Delivery
  - Tunneling or routing?
- Recovery Process (reverse redirection)
  - Conditions - ToS? Duration? Priority? Capacity?

Mitigation On Premise

- On premise - in front of your firewall, WAF, etc.; typically in a L2 config transparent to traffic and deployed at enterprise location or data center
- May incorporate some level of SSL decryption / inspection. Radware uses an external ADC (load balancer) with SSL acceleration cards here.
- On premise units are still vulnerable to pipe saturation, so some level of “signaling” to external orchestration is needed to determine when to redirect traffic. Radware offers proprietary signaling, but netflow / openflow from a router can also indicate saturation.
- Using on premise with a cloud as backup is sometimes called “hybrid”. With hybrid the on premise handles the load until it's too big and then invokes the scrubbing center but still does more complex mitigations

Mitigation – Scrubbing Center or Cloud

- Can back up an on-premise solution or be the main strategy
- Scrubbing Center (in carrier) or Cloud provider relies on routing or DNS changes described before
- Scrubbing Center is L3 - it has an IP. Mitigation box can be L2 or L3
  - One method - Multiple scrubbing centers off regional routers with the same IP
  - Edge routers push traffic across the L3 interfaces on the DDoS box using ECMP
  - Many centers are now incorporating an orchestration layer so traffic can be mitigated closest to the source and each scrubbing center does have its own IP. With virtualization, you can spin up lots of lower capacity but effective scrubbing or detection machines.
- Per box capacities ranging up to 300-400 Gbps, per center many strive for 1 Tbps and higher

Mitigation Protection Types

- Blacklist by country or other
- Active (ex: TCP RST)
- Passive (DNS no-response)
- DNS record whitelisting
- DNS response whitelisting
- Thresholds by message type (from or to specific IPs)
- Behavioral – fingerprinting repeated patterns
- SSL decryption via card or separate appliance
- Signaling, black hole routing

Resources

- Cheat Sheet and AppDDoS Script https://github.com/unregistered436/DDoS

- Look at https://github.com/markus-go/bonesi - Spoofed TCP tool written in C, so faster than my script

- Monitor your network interfaces: http://www.binarytides.com/linux-commands-monitor-network/